I CLAIM:

1. A computing device-implemented method for carrying out encryption using a key value for encrypting a plaintext value to define a cipher text, the encryption being defined using an encryption function, the method comprising the steps of:
   a) defining a masked encryption function by masking the encryption function using an encryption function mask value;
   b) defining a set of more than one split mask values, at least one of the set of split mask values being defined with reference to the encryption function mask value;
   c) generating a final mask value by masking the key value using masking steps that comprise masking by applying the set of split mask values;
   d) determining an input value by masking the plaintext value using masking steps that comprise masking by applying the fixed final mask value; and
   e) applying the input value to the encryption function to provide a cipher text output.
2. The method of claim 1 in which

   the step of generating the final mask value further comprises the step of masking the key value using a key mask value prior to masking with the set of split mask values, and which

   further comprises the step of using the key mask value as a mask, as part of the step of defining one of the values in the set of split mask values with reference to the encryption function mask value.
3. The method of claim 2 in which the step of defining one of the set of split mask values with reference to the encryption function mask value further comprises the steps of masking the said split mask value with the other values in the set of split mask values.
4. The method of claim of claim 2 in which the step of defining a set of split mask values m1...mn comprises the steps of:
   a) defining the encryption function mask value to comprise a set of random values $m_{in}1$ to $m_{in}n$;
   b) defining the set of split mask values to be the random values m1 to mn-1; and

c) defining a masking value mn in the set of split mask values to be (key mask value)^ $m_{in}1$^...^$m_{in}n$^m1^...^mn-1.

5. The method of claims 1, 2, 3, or 4, in which the encryption function is a table look-up.
6. The method of claims 1, 2, 3, 4, or 5 in which masking is a bitwise exclusive or operation carried out on binary values.
7. The method of claim 2 further comprising the step of storing the masked key and the set of split mask values.
8. The method of claims 2, 3, 4, 5, or 6 further comprising the steps of applying a random mask to an even number of the set of split mask values prior to the step of masking the key value with the set of split mask values.
9. A countermeasure method for resisting security attacks on a processing unit using a key to perform a defined cryptographic function, the method comprising the following steps:

a) obtaining the key and a random value r;

b) obtaining a set of n random input values $m_{in}1$, ... $m_{in}n$;

c) defining a masked function by masking the defined cryptographic function with the value $m_{in}1$^...^$m_{in}n$;

d) masking the key with the random value r to define the value mkey;

e) obtaining a set of random values m1, ... mn-1;

f) defining a value mn to be r^$m_{in}1$^...^$m_{in}n$^m1^...^mn-1; and

g) using the values m1,...,mn and mkey to define input for the masked function.

10. The method of claim 9 in which the encryption function is a table look-up.
11. The method of claims 9 or 10 in which masking is a bitwise exclusive or operation carried out on binary values.

12. A countermeasure method for resisting security attacks on a processing unit using a key to encrypt a plaintext value using a look up on a table, the method comprising the following steps:

a) obtaining the key and a random value r;

b) obtaining a set of n random input values $m_{in}1$, ... $m_{in}n$;

c) defining a masked table by masking the defined look-up table with the value $m_{in}1$^...^$m_{in}n$;

d) masking the key with the random value r to define the value mkey;

e) obtaining a set of random values m1, ... mn-1;

f) defining a value mn to be r^$m_{in}1$^...^$m_{in}n$^m1^...^mn-1; and

g) masking the plaintext with the values m1,...,mn and mkey to define input for the masked table.

13. The method of claim 12 in which masking is a bitwise exclusive or operation carried out on binary values.

14. A computing device-implemented method for use in a cryptographic process, the cryptographic process using a key value to define input to a cryptographic function, the method comprising the steps of:

a) masking the cryptographic function using a function mask value;

b) defining a set of more than one split mask values, at least one of the set of split mask values being defined with reference to the function mask value;

c) masking the key value using steps that comprise masking by applying the set of split mask values to obtain a masked input key value; and

d) using the masked input key value to define the input to the masked cryptographic function.

15. The method of claim 14, further comprising the step of randomizing the split mask values.

16. A computing device-implemented method for use with an AES key generation process for defining masked round keys for use in AES encryption, the method comprising the steps of:

a) defining a masked table for use the AES key generation process using table mask M;

b) defining a set of four split mask values, one of the set of split mask values being defined with relation to table mask M;

c) masking a set of four key values using the set of four split mask values and applying the resulting values to the AES key generation process using the masked table and a set of intermediate mask values whereby the set of AES round keys defined using table look-up are defined by applying an appropriate intermediate mask value to the input value for the masked table; and

d) masking the round keys produced by the AES key generation process by applying an appropriate intermediate mask value to the round keys that are not directly defined using table look-up.

17. The method of claim 16 in which the four key values are each masked with one of a set of four key mask values and in which the split mask value in the set of split key mask values that is defined with relation to table mask M is further masked with each of the four key mask values.

18. The method of claim 16 in which the key mask values are specified as n0, n1, n2, n3 and the split mask values are specified as m0, m1, m2, m3 and in which m0, m1, m2 are randomly defined and m3 is defined to be M^n0^n1^n2^n3^m0^m1^m2.

19. The method of claim 18 further comprising the step of masking m0 and m1 with a first random value and masking m2 and m3 with a second random value.

20. A computing device-implemented method for carrying out AES encryption using the round keys as defined in claim 16, the output of the AES encryption being unmasked using the key mask values and the split mask values.

21. The method of claim 20 in which the unmasking is carried out in more than one step such that the key mask values and the split mask values are not combined so as to produce a single unmasking value.

22. A computing device program product for carrying out encryption using a key value for encrypting a plaintext value to define a cipher text, the encryption being defined using an encryption function, the computing device program product comprising a computer usable medium having computer readable program code means embodied in said medium, and comprising

program code means for defining a masked encryption function by masking the encryption function using an encryption function mask value;

program code means for defining a set of more than one split mask values, at least one of the set of split mask values being defined with reference to the encryption function mask value;

program code means for generating a final mask value by masking the key value using masking steps that comprise masking by applying the set of split mask values;

program code means for determining an input value by masking the plaintext value using masking steps that comprise masking by applying the fixed final mask value; and

program code means for applying the input value to the encryption function to provide a cipher text output.

23. The computing device program product of claim 22 in which

the program code means for generating the final mask value further comprises program code means for masking the key value using a key mask value prior to masking with the set of split mask values, and which

further comprises program code means for using the key mask value as a mask, as part of defining one of the values in the set of split mask values with reference to the encryption function mask value.

24. The computing device program product of claim 23 in which the program code means for defining one of the set of split mask values with reference to the encryption function mask value further comprises program code means for masking the said split mask value with the other values in the set of split mask values.

25. The computing device program product of claim 23 in which the program code means for defining a set of split mask values m1...mn comprises program code means for:

a) defining the encryption function mask value to comprise a set of random values $m_{in}1$ to $m_{in}n$,

b) defining the set of split mask values to be the random values m1 to mn-1; and

c) defining a masking value mn in the set of split mask values to be (key mask value)^ $m_{in}1$^...^$m_{in}n$^m1^...^mn-1.

26. The computing device program product of claims 22, 23, 24, or 25 in which the encryption function is a table look-up.

27. The computing device program product of claims 22, 23, 24, 25 or 26 in which masking is a bitwise exclusive or operation carried out on binary values.

28. The computing device program product of claim 23 further comprising program code means for storing the masked key and the set of split mask values.

29. The computing device program product of claims 23, 24, 25, 26 or 27 further comprising program code means for applying a random mask to an even number of the set of split mask values prior to masking the key value with the set of split mask values.

30. A computing device program product for resisting security attacks on a processing unit using a key to perform a defined cryptographic function, the computing device program product comprising a computer usable medium having computer readable program code means embodied in said medium, and comprising

program code means for obtaining the key and a random value r,

program code means for obtaining a set of n random input values $m_{in}1$, ... $m_{in}n$,

program code means for defining a masked function by masking the defined cryptographic function with the value $m_{in}1$^...^$m_{in}n$,

program code means for masking the key with the random value r to define the value mkey,

program code means for obtaining a set of random values m1, ... mn-1,

program code means for defining a value mn to be
r^m_{in}1^...^m_{in}n^m1^...^mn-1, and

program code means for using the values m1,...,mn and mkey to define input for the masked function.

31. The computing device program product of claim 30 in which the encryption function is a table look-up.
32. The computing device program product of claims 30 and 31 in which masking is a bitwise exclusive or operation carried out on binary values.
33. A computing device program product for resisting security attacks on a processing unit using a key to encrypt a plaintext value using a look up on a table, the computing device program product comprising a computer usable medium having computer readable program code means embodied in said medium, and comprising

program code means for obtaining the key and a random value r,

program code means for obtaining a set of n random input values m_{in}1, ... m_{in}n,

program code means for defining a masked table by masking the defined look-up table with the value m_{in}1^...^m_{in}n,

program code means for masking the key with the random value r to define the value mkey,

program code means for obtaining a set of random values m1, ... mn-1,

program code means for defining a value mn to be
r^m_{in}1^...^m_{in}n^m1^...^mn-1, and

program code means for masking the plaintext with the values m1,...,mn and mkey to define input for the masked table.

34. The computing device program product of claim 33 in which masking is a bitwise exclusive or operation carried out on binary values.

35. A computing device program product for use in a cryptographic process, the cryptographic process using a key value to define input to a cryptographic function, the computing device program product comprising a computer usable medium having computer readable program code means embodied in said medium, and comprising

program code means for masking the cryptographic function using a function mask value,

program code means for defining a set of more than one split mask values, at least one of the set of split mask values being defined with reference to the function mask value,

program code means for masking the key value using steps that comprise masking by applying the set of split mask values to obtain a masked input key value,

program code means for using the masked input key value to define the input to the masked cryptographic function.

36. The computing device program product of claim 35, further comprising program code means for randomizing the split mask values.

37. A computing device program product for use with an AES key generation process for defining masked round keys for use in AES encryption, the computing device program product comprising a computer usable medium having computer readable program code means embodied in said medium, and comprising

program code means for defining a masked table for use the AES key generation process using table mask M,

program code means for defining a set of four split mask values, one of the set of split mask values being defined with relation to table mask M,

program code means for masking a set of four key values using the set of four split mask values and applying the resulting values to the AES key generation process using the masked table and a set of intermediate mask values whereby

the set of AES round keys defined using table look-up are defined by applying an appropriate intermediate mask value to the input value for the masked table program code means for masking the round keys produced by the AES key, and

generation process by applying an appropriate intermediate mask value to the round keys that are not directly defined using table look-up.

38. The computing device program product of claim 37 further comprising program code means for masking the four key values with a set of four key mask values and for further masking the split mask value in the set of split key mask values that is defined with relation to table mask M with each of the four key mask values.

39. The computing device program product of claim 37 in which the key mask values are specified as n0, n1, n2, n3 and the split mask values are specified as m0, m1, m2, m3 and comprising program code means for randomly defining m0, m1, m2 and defining m3 to be M^n0^n1^n2^n3^m0^m1^m2.

40. The computing device program product of claim 39 further comprising program code means for masking m0 and m1 with a first random value and masking m2 and m3 with a second random value.

41. A computing device program product for carrying out AES encryption using the round keys as defined in claim 37, the computing device program product comprising a computer usable medium having computer readable program code means embodied in said medium, and comprising program code means for unmasking the output of the AES encryption using the key mask values and the split mask values.

42. The computing device program product of claim 41 in which the program code for unmasking comprises code for unmasking in more than one step such that the key mask values and the split mask values are not combined so as to produce a single unmasking value.

43. A system for carrying out encryption using a key value for encrypting a plaintext value to define a cipher text, the encryption being defined using an encryption function, the system comprising

means for defining a masked encryption function by masking the encryption function using an encryption function mask value;

means for defining a set of more than one split mask values, at least one of the set of split mask values being defined with reference to the encryption function mask value;

means for generating a final mask value by masking the key value using masking steps that comprise masking by applying the set of split mask values;

means for determining an input value by masking the plaintext value using masking steps that comprise masking by applying the fixed final mask value; and

means for applying the input value to the encryption function to provide a cipher text output.

44. The system of claim 43 in which

the means for generating the final mask value further comprises means for masking the key value using a key mask value prior to masking with the set of split mask values, and which system

further comprises means for using the key mask value as a mask, as part of defining one of the values in the set of split mask values with reference to the encryption function mask value.

45. The system of claim 44 in which the means for defining one of the set of split mask values with reference to the encryption function mask value further comprises means for masking the said split mask value with the other values in the set of split mask values.

46. The system of claim 44 in which the means for defining a set of split mask values m1...mn comprises means for

a) defining the encryption function mask value to comprise a set of random values $m_{in}1$ to $m_{in}n$;

b) defining the set of split mask values to be the random values m1 to mn-1; and

c) defining a masking value mn in the set of split mask values to be (key mask value)^ $m_{in}1$^...^$m_{in}n$^m1^...^mn-1.

47. The system of claims 43, 44, 45 or 46, in which the encryption function is a table look-up.

48. The system of claims 43, 44, 45, 46 or 47 in which masking is a bitwise exclusive or operation carried out on binary values.

49. The system of claim 44 further comprising means for storing the masked key and the set of split mask values.

50. The system of claims 44, 45, 46, 47 or 48 further comprising means for applying a random mask to an even number of the set of split mask values prior to masking the key value with the set of split mask values.

51. A system for use in a cryptographic process, the cryptographic process using a key value to define input to a cryptographic function, the system comprising

means for masking the cryptographic function using a function mask value;

means for defining a set of more than one split mask values, at least one of the set of split mask values being defined with reference to the function mask value;

means for masking the key value using steps that comprise masking by applying the set of split mask values to obtain a masked input key value; and

means for using the masked input key value to define the input to the masked cryptographic function.

52. The system of claim 51, further comprising means for randomizing the split mask values.

53. A system for use with an AES key generation process for defining masked round keys for use in AES encryption, the system comprising

means for defining a masked table for use the AES key generation process using table mask M,

means for defining a set of four split mask values, one of the set of split mask values being defined with relation to table mask M.

means for masking a set of four key values using the set of four split mask values and applying the resulting values to the AES key generation process using the masked table and a set of intermediate mask values whereby the set of AES round keys defined using table look-up are defined by applying an

appropriate intermediate mask value to the input value for the masked table, and

means for masking the round keys produced by the AES key generation process by applying an appropriate intermediate mask value to the round keys that are not directly defined using table look-up.

54. The system of claim 53 further comprising means for masking the four key values with a set of four key mask values and for further masking the split mask value in the set of split key mask values that is defined with relation to table mask M with each of the four key mask values.

55. The system of claim 53 in which the key mask values are specified as n0, n1, n2, n3 and the split mask values are specified as m0, m1, m2, m3 and comprising means for randomly defining m0, m1, m2 and defining m3 to be M^n0^n1^n2^n3^m0^m1^m2.

56. The system of claim 55 further comprising means for masking m0 and m1 with a first random value and masking m2 and m3 with a second random value.

57. A system for carrying out AES encryption using the round keys as defined in claim 53, the computing device program product comprising a computer usable medium having computer readable means embodied in said medium, and comprising means for unmasking the output of the AES encryption using the key mask values and the split mask values.

58. The system of claim 57 in which the program code for unmasking comprises code for unmasking in more than one step such that the key mask values and the split mask values are not combined so as to produce a single unmasking value.